

FINITE 2-GROUPS WITH ODD NUMBER OF CONJUGACY CLASSES

ANDREI JAIKIN-ZAPIRAIN AND JOAN TENT

ABSTRACT. In this paper we consider finite 2-groups with odd number of real conjugacy classes. On one hand we show that if k is an odd natural number less than 24, then there are only finitely many finite 2-groups with exactly k real conjugacy classes. On the other hand we construct infinitely many finite 2-groups with exactly 25 real conjugacy classes. Both results are proven using pro- p techniques and, in particular, we use the Kneser classification of semi-simple p -adic algebraic groups.

1. INTRODUCTION

We recall that an element in a group G is **real** if it is conjugate in G to its inverse, and a conjugacy class of G is **real** if it consists of real elements. It is well known that certain conditions on the set of real conjugacy classes of a finite group may strongly influence the structure of the group, the first example of this possibly being that a finite group contains no non-trivial real conjugacy classes if and only if it has odd order. In the present paper we study finite 2-groups satisfying a particular condition of this nature, namely that its number of real conjugacy classes is an odd natural number.

A theorem by M. Isaacs, G. Navarro and J. Sangroniz [6] characterizes the finite 2-groups of maximal class as those possessing precisely 5 rational-valued irreducible characters. It is easy to see that if a 2-group has 5 real irreducible characters, then all of them are rational-valued, and thus the group has maximal class. As a consequence of this, it is deduced in [6] that there are (up to isomorphism) only 3 finite 2-groups with 5 real conjugacy classes, all of them having maximal class. Now, a considerably easier fact is that there are no 2-groups with 3 real conjugacy classes. As a continuation of these results, it is proved in [12] that a finite 2-group with 7 real classes has order at most 128.

Indeed, it is a relevant observation that most 2-groups of small order appear to have an even number of conjugacy classes. Since the real classes in a (finite) group are those classes fixed by the action induced by inversion of elements, it is clear that the parity of the number of conjugacy classes of a finite group coincides with the parity of the number of its real classes. Then most small 2-groups have an even number of real conjugacy classes. In order to explain this phenomenon, Josu Sangroniz proposed the following conjecture [12], which motivates our work.

2000 *Mathematics Subject Classification.* Primary 20D15 ; Secondary 20C15, 20E45, 20E18.

Key words and phrases. 2-groups, real classes, p -adic groups.

This paper is partially supported by the grant MTM 2011-28229-C02-01 and MTM2014-53810-C2-01 of the Spanish MEyC and by the ICMAT Severo Ochoa project SEV-2011-0087. The second author has also been supported by PROMETEOII/2015/011.

Conjecture. *If r is an odd natural number, then there are only finitely many finite 2-groups with exactly r real conjugacy classes.*

Our purpose in this paper is to give an answer to this problem. More precisely, we shall confirm the conjecture for $r \leq 23$ and show that it is false when $r = 25$.

Theorem A. *Let $r \leq 23$ be an odd natural number. Then there are only finitely many finite 2-groups with exactly r real conjugacy classes.*

Theorem B. *There are infinitely many finite 2-groups with exactly 25 real conjugacy classes.*

In contrast to the previous results for 2-groups with an odd number $r \leq 7$ of real conjugacy classes, which are obtained by methods of finite group theory and its representation theory, both Theorem A and Theorem B are proven using pro- p techniques, as we next briefly sketch.

It turns out that the existence of infinitely many finite 2-groups with exactly k real classes is equivalent to the existence of an infinite pro-2 group such that almost all its finite quotients have exactly k real classes. Consequently, the problem is reduced to the study of such pro-2 groups. As we shall prove, these groups have finite rank, and so they are 2-adic analytic. These key steps in our reduction of the problem require to use a basic property of the real classes in a finite group, which is that its number coincides with the number of real-valued irreducible characters of the group. In fact, one advantage of passing from conjugacy classes to characters is that the latter behave better with respect to quotient groups, and this is exploited in the construction of a pro-2 group with k real classes. On the other hand, we shall need to look at the real conjugacy classes again in order to control the rank of this pro-2 group.

When the number of real conjugacy classes k is odd, we shall show that our analysis should be focused on a Sylow pro-2 group of the automorphism group of a semi-simple Lie \mathbb{Q}_2 -algebra. These groups are well understood, because of the classification of semi-simple p -adic algebraic groups by M. Kneser [9], which therefore plays an essential role in the proof of Theorem A. It is certainly remarkable that the proof of our result on real classes of finite 2-groups needs an appeal to this deep result from the theory of algebraic groups. It is ultimately M. Kneser's classification which indicates us where to look for a minimal counterexample to the conjecture, and as a matter of fact the groups in Theorem B are finite quotients of a Sylow pro-2 group of $\mathrm{PGL}_1(D)$, where D is a division \mathbb{Q}_2 -algebra of dimension 9 (we recall that up to isomorphism there are only two such algebras, both of them having isomorphic multiplicative groups).

We note that the fact that the equality between the number of real classes and the number of real characters in a finite group in general has no analogue in the case of rational values, seems to be an obstruction to apply our arguments in a rather direct way to related questions on rational classes and characters in finite 2-groups. On the contrary, by this same reason our methods may be valid for similar problems concerning fields of values in 2-groups in which equality holds, as it is the case of the field $\mathbb{Q}(i)$, being the fixed field of a cyclic Galois group acting on the classes of a finite 2-group.

Acknowledgements. We would like to thank Josu Sangroniz for useful comments on preliminary versions of this paper.

2. FINITE GROUP PRELIMINARIES

In this section we include some preliminary results about real classes of finite groups which we shall need later on.

Let a group H act on a group G as automorphisms. We will usually consider the action of a subgroup H of G on G by conjugation, and the induced action on quotients of G . By a slight abuse of language, we may call the orbits of the action H -conjugacy classes. For a subset T of G , we denote by $k_H(T)$ the number of H -orbits in G that have non-trivial intersection with T . If G acts on itself by conjugation, then for simplicity $k(G) = k_G(G)$ will denote the number of conjugacy classes of G . An element $g \in G$ is called H -**real**, or simply **real** when there is no possible confusion, if g and g^{-1} are in the same H -orbit. A conjugacy class is called H -real if it consists of H -real elements. We denote by $r_H(T)$ the number of H -real conjugacy classes of G that have non-trivial intersection with T . For simplicity we write $r(G) = r_G(G)$.

In the Introduction we already noted that the parities of $k(G)$ and $r(G)$ coincide when G is a finite group. Next we prove this easy fact.

Lemma 2.1. *For a finite group G , $k(G) \equiv r(G) \pmod{2}$.*

Proof. Observe that inversion of elements in G induces a permutation of order at most 2 on the set of conjugacy classes of G . Since a conjugacy class of G is real if and only if it is fixed by this permutation, the result is clear. \square

The following results relate the parities of the number of conjugacy classes of a finite 2-group and a maximal subgroup of it.

Lemma 2.2. *Let H be a subgroup of a finite group G of index 2. Then $k(H) \equiv k_G(G \setminus H) \pmod{2}$.*

Proof. Recall that if G acts on a non-empty finite set Ω , then by Burnside's formula ([16, Theorem 3.22]), the number of orbits of the action equals to

$$\frac{1}{|G|} \sum_{g \in G} |\text{Fix}_\Omega(g)|,$$

where $\text{Fix}_\Omega(g)$ is the set of fixed points of $g \in G$ in Ω . Since both H and $G \setminus H$ are normal subsets of G we have that

$$\begin{aligned} 2k_G(H) &= \frac{2}{|G|} |\{(g, h) \in G \times H : gh = hg\}| \\ &= k_H(G) = k_H(G \setminus H) + k(H) = k_G(G \setminus H) + k(H), \end{aligned}$$

where the last equality follows from the fact that each G -conjugacy class in $G \setminus H$ is already an orbit under conjugation by H , because H has index 2 in G . \square

Corollary 2.3. *Let G be a finite group and H a subgroup of index 2. If there are no real elements in $G \setminus H$, then $k(H)$ is even.*

If G is a finite group, we denote by $\text{Irr}(G)$ the set of irreducible complex characters of G . If \bar{G} is a quotient group of G then $\text{Irr}(\bar{G})$ is identified in a natural way with a subset of $\text{Irr}(G)$. We denote by $\text{Irr}_r(G)$ the set of irreducible characters of G taking only real values. Such characters are called **real**.

Lemma 2.4. *For a finite group G , $r(G) = |\text{Irr}_r(G)|$.*

Proof. This is an immediate consequence of Brauer's Theorem 6.32 of [5] (see Problem 6.13 of [5]). \square

As a consequence of the previous lemma and the fact that characters of a quotient group can be identified with characters of the whole group, we obtain the following:

Corollary 2.5. *Let G be a finite group having r real conjugacy classes. Then any quotient group of G has at most r real conjugacy classes.*

In the next proposition we compare the number of real classes in H and $G \setminus H$ when H has index 2 in a finite group G .

Proposition 2.6. *Let G be a finite group and H a subgroup of G of index 2. Denote by $\text{Irr}_{r,G}(H)$ the set of real irreducible characters of H which are G -invariant. Then*

$$r_G(G \setminus H) \leq |\text{Irr}_{r,G}(H)|.$$

In particular, $r_G(G \setminus H) \leq r(H)$.

Proof. Let $\varphi \in \text{Irr}(H)$ be such that there exists $\chi \in \text{Irr}_r(G)$ lying over φ , so $\overline{\varphi} \in \text{Irr}(H)$ is also a constituent of χ_H . Since G/H is cyclic, φ is G -invariant if and only if $\chi_H = \varphi$ by Corollary 11.22 of [5], so φ is real-valued in this case. Also, Gallagher's theorem [5, Corollary 6.17] implies that if φ is G -invariant then φ has 2 irreducible extensions to G , both of them being real-valued because χ is real. On the other hand, if φ is not G -invariant then $\chi_H = \varphi + \varphi^a$, where $a \in G \setminus H$, and χ is the only irreducible character of G lying over φ , by Clifford's correspondence [5, Theorem 6.11]. For any $a \in G \setminus H$, this yields to

$$\begin{aligned} |\text{Irr}_r(G)| &\leq 2|\text{Irr}_{r,G}(H)| + \frac{|\text{Irr}_r(H) \setminus \text{Irr}_{r,G}(H)|}{2} + \frac{|\{\varphi \in \text{Irr}(H) : \varphi^a = \overline{\varphi} \neq \varphi\}|}{2} \\ &= \frac{3|\text{Irr}_{r,G}(H)|}{2} + \frac{|\text{Irr}_r(H)|}{2} + \frac{|\{\varphi \in \text{Irr}(H) : \varphi^a = \overline{\varphi} \neq \varphi\}|}{2}. \end{aligned}$$

Since $|\{\varphi \in \text{Irr}(H) : \varphi^a = \overline{\varphi}\}| = |\text{Irr}_{r,G}(H)| + |\{\varphi \in \text{Irr}(H) : \varphi^a = \overline{\varphi} \neq \varphi\}|$, we obtain that

$$(2.1) \quad |\text{Irr}_r(G)| \leq |\text{Irr}_{r,G}(H)| + \frac{|\text{Irr}_r(H)|}{2} + \frac{|\{\varphi \in \text{Irr}(H) : \varphi^a = \overline{\varphi}\}|}{2}.$$

Now, denote by $r^G(H)$ the number of real conjugacy classes of H which are stabilized by G under conjugation. If $K = Cl_H(x)$ for $x \in H$, we write $K^{-1} = Cl_H(x^{-1})$ and $K^a = Cl_H(x^a)$, where again $a \in G \setminus H$. For any $a \in G \setminus H$, it is clear that

$$\begin{aligned} r_G(H) &= r^G(H) + \frac{1}{2}(r(H) - r^G(H)) + \frac{1}{2}|\{K \in Cl(H) : K^a = K^{-1} \neq K\}| \\ &= \frac{1}{2}r(H) + \frac{1}{2}r^G(H) + \frac{1}{2}|\{K \in Cl(H) : K^a = K^{-1} \neq K\}|. \end{aligned}$$

Note that

$$|\{K \in Cl(H) : K^a = K^{-1}\}| = r^G(H) + |\{K \in Cl(H) : K^a = K^{-1} \neq K\}|,$$

and so

$$(2.2) \quad r_G(H) = \frac{r(H)}{2} + \frac{|\{K \in Cl(H) : K^a = K^{-1}\}|}{2}.$$

Let an involution σ act on the sets $\text{Irr}(H)$ and $\text{Cl}(H)$ via $\varphi^\sigma = \overline{\varphi^a}$ and $K^\sigma = (K^a)^{-1}$, respectively, for all $\varphi \in \text{Irr}(H)$ and $K \in \text{Cl}(H)$. By Brauer's Theorem 6.32 of [5], σ fixes the same number of points in $\text{Irr}(H)$ that in $\text{Cl}(H)$, that is

$$|\{\varphi \in \text{Irr}(H) : \varphi^a = \overline{\varphi}\}| = |\{K \in \text{Cl}(H) : K^a = K^{-1}\}|.$$

Since by Lemma 2.4, $|\text{Irr}_r(H)| = r(H)$ and $|\text{Irr}_r(G)| = r(G) = r_G(H) + r_G(G \setminus H)$, it follows from (2.1) and (2.2) that

$$r_G(G \setminus H) \leq |\text{Irr}_{r,G}(H)| \leq |\text{Irr}_r(H)| = r(H).$$

□

For a finite 2-group G , we consider the following series of subgroups:

$$G_1 = G, \quad G_{k+1} = [G_k, G]G_k^2 \quad (k \geq 1).$$

Note that the series eventually reaches the trivial subgroup $\{1_G\}$, because G is nilpotent. For simplicity instead of “bounded by a function that only depends on r ” we shall write simply “ r -bounded”. Recall that the **rank** of a finite group is the supremum of the number of generators of its subgroups. (Of course, it is understood that the number of generators of a group G is the size of a minimal generating set of G .)

Lemma 2.7. *Let G be a finite 2-group with r real conjugacy classes. Then the following holds:*

- (1) *The number of conjugacy classes of elements of order 2 in every quotient group of G is r -bounded.*
- (2) *The rank of G is r -bounded.*
- (3) *There exists a r -bounded number k such that $\text{Irr}_r(G) \subseteq \text{Irr}(G/G_k)$.*

Proof. Involutions are real elements, because an element of order 2 is its own inverse, so (1) follows from Corollary 2.5. Now (2) follows from (1) and exercise 7 of Chapter 2 in [3]. Finally, by [12, Theorem C], there exists a normal subgroup N of G of r -bounded index in G such that $\text{Irr}_r(G) \subseteq \text{Irr}(G/N)$. Thus (3) follows from the nilpotency of G . □

3. PROFINITE GROUP PRELIMINARIES

In this section we extend some of the results about real characters and real classes from the previous section to profinite groups.

If P is a profinite group we denote by $\text{Irr}(P)$ the set of irreducible continuous complex characters of P , i.e. $\text{Irr}(P)$ is the union of $\text{Irr}(\bar{P})$ for all the finite continuous quotients \bar{P} of P . As in the finite order case, we denote by $\text{Irr}_r(P)$ the subset of characters of $\text{Irr}(P)$ taking only real values. We say that a profinite group P is **\mathbb{R} -finite** if the set $\text{Irr}_r(P)$ is finite. It is not true in general that for a profinite group P the number of conjugacy classes of real elements is equal to the cardinality of $\text{Irr}_r(P)$, as it is the case for finite groups. For example, in a non-abelian free pro-2 group the trivial element forms the unique real conjugacy class, but the number of real irreducible characters is infinite.

Lemma 3.1. *Let P be a profinite group. Then the following holds.*

- (1) *An element $g \in P$ is real if gN is real in P/N for any open normal subgroup N of P .*

- (2) Let \mathcal{S} be a closed subset of P , S the set of P -real elements of \mathcal{S} and N a normal open subgroup of P . Then there exists a normal open subgroup L of P contained in N such that the P/L -real elements of SL/L lie in SN/L ;
- (3) $|\text{Irr}_r(P)| = \sup_{N \trianglelefteq_o P} |\text{Irr}_r(P/N)|$.
- (4) If P is \mathbb{R} -finite, then it has at most $|\text{Irr}_r(P)|$ real conjugacy classes. In particular, every real element of P has finite order in this case.

Proof. First we prove (1). Suppose that gN is real in P/N for all open normal subgroups N of P , and define $X_N = \{x \in P \mid (gN)^x = (gN)^{-1}\} \neq \emptyset$ for each $N \trianglelefteq_o P$. Note that $\{X_N\}_{N \trianglelefteq_o P}$ is an inverse system of compact sets with the inclusion maps, since $X_N \subseteq X_M$ if $N \subseteq M$ and $N, M \trianglelefteq_o P$. Then the inverse limit of this inverse set is non-empty ([14, Proposition 1.1.4]), so there exists $x \in P$ such that $gg^x \in N$ for all $N \trianglelefteq_o P$, and thus $g^x = g^{-1}$, as wanted.

We work by contradiction in order to obtain (2). For each open normal subgroup L of P contained in N , let X_L be the set of elements $x \in SL$ such that xL is real in P/L but $x \notin SN$, and suppose that $X_L \neq \emptyset$ for each such L . Since the set formed by such subgroups L is a base of neighborhoods of the identity element, SN is open and \mathcal{S} is closed, arguing as in (1) it follows that there exists a real element in \mathcal{S} not lying in SN , which of course is a contradiction.

Note that (3) follows from the definition of $\text{Irr}(P)$, and the first part of (4) follows from (3), Lemma 2.4 and the fact that two elements $x, y \in P$ are conjugate in P if and only if xN, yN are conjugate for any open normal subgroup N of P .

Finally, suppose that P is \mathbb{R} -finite and $x \in P$ is real of infinite order, so $M_x = \{o(xN) \mid N \trianglelefteq_o P\}$ is infinite. Thus there exist infinitely many $m \in \mathbb{N}$ such that $x \notin N_m$ and $x^m \in N_m$ for some $N_m \trianglelefteq_o P$ depending on m , which implies that x is not conjugate to x^m . Similarly, x^m is not conjugate to x^n if $n, m \in M_x$ with $n \neq m$. Since powers of real elements are real, P has infinitely many real classes, which is a contradiction. \square

The following corollary is a consequence of the previous lemma and Corollary 2.3.

Corollary 3.2. *Let Q be a profinite group and P an open subgroup of index 2. Assume that there are no real elements of Q in $Q \setminus P$. Then there exists an open normal subgroup L of Q contained in P such that for any normal open subgroup M of Q contained in L , $r(P/M) \equiv 0 \pmod{2}$. Thus if $|\text{Irr}_r(P)|$ is finite, then it is even.*

4. \mathbb{R} -FINITE PRO-2 GROUPS AND PRO 2-GROUPS OF FINITE RANK

In this section we include some basic facts about pro- p groups of finite rank and analyze their real characters and real classes.

Let P be a profinite group. Denote by $d(P)$ the minimal cardinality of a topological generating set of P (see [3, p. 20]). Then the **rank** of P is defined to be the supremum of $d(H)$, where H ranges over the closed subgroups of P . Pro- p groups of finite rank are very well understood, and we refer the reader to [3] for different equivalent characterizations of this class of groups. We say that a finitely generated pro- p group N is **uniform** if N is torsion-free and $[N, N] \leq N^{2p}$. It is a fundamental result that the pro- p groups of finite rank are exactly the virtually uniform pro- p groups, that is the pro- p groups having a (normal) uniform subgroup U of finite index. From this we immediately obtain that a pro- p group P of finite

rank has a unique maximal finite normal subgroup, denoted $\text{rad}_f(P)$. In fact, one can obtain a stronger result.

Lemma 4.1. *Let P be a pro- p group of finite rank. Then there are only finitely many conjugacy classes of finite subgroups in P .*

Proof. See Theorem 4.23 of [3]. \square

Suppose that P is a finitely generated pro-2 group. As in the finite order case, consider the following series of subgroups of P :

$$P_1 = P, \quad P_{k+1} = [P_k, P]P_k^2 \quad (k \geq 1).$$

If N is a uniform pro-2 group, then $N_k = N^{2^k}$ and $\{N_k\}_{k \in \mathbb{N}}$ is a base of open neighbourhoods of the identity.

In the next lemma we collect some basic properties of \mathbb{R} -finite pro-2 groups.

Lemma 4.2. *Let P be a \mathbb{R} -finite pro-2 group. Then the following holds.*

- (1) P has finite rank;
- (2) there exists a normal open subgroup N of P such that N is uniform and $\text{Irr}_r(P) \subseteq \text{Irr}(P/N)$;
- (3) any element of P of finite order belongs to $\text{rad}_f(P)$.

Proof. The first two propositions follow from Lemma 2.7 (2,3). In order to show (3) it is enough to prove that if $\text{rad}_f(P) = \{1\}$, then P is torsion free. Thus, assume that $\text{rad}_f(P) = \{1\}$ and that there exists $x \in P$ of order 2. Let N be a uniform normal open subgroup of P . Then, since the elements of the form $[x, g]$ with $g \in N$ are inverted by x , we have that they have finite order by Lemma 3.1 (4). On the other hand, $[x, N] \leq N$ and N is torsion free, so $x \in C_P(N)$. Now since N has finite index in P , then $C_P(N)$ is virtually central. Hence its derived subgroup is finite, by Schur's theorem [15, Theorem 10.1.4]. Since $\text{rad}_f(C_P(N)) \leq \text{rad}_f(P) = \{1\}$, we deduce that $C_P(N)$ is abelian. Thus $x \in \text{rad}_f(C_P(N)) = \{1\}$, a contradiction. \square

Thus, in order to understand \mathbb{R} -finite pro-2 groups we have to look at pro-2 groups of finite rank. The most powerful method to study these groups is based on the Lie method that we describe next.

Let L be a Lie \mathbb{Z}_p -algebra. We say that L is **uniform** if for some k , $L \cong \mathbb{Z}_p^k$ as a \mathbb{Z}_p -module and $[L, L] \subseteq 2pL$. One can define the functors **exp** and **log** between the categories of uniform Lie \mathbb{Z}_p -algebras and uniform pro- p -groups in such a way that these two functors are isomorphisms of categories (see [3, Chapter 4]). There is a relatively easy way to define the functor **log**. If N is a uniform pro- p group, then every element $x \in N^{p^i}$ has a unique p^i th root in N , denoted x^{1/p^i} . Now **log**(N) is defined to be the Lie \mathbb{Z}_p -algebra whose underlying set coincides with N , and which has Lie operations defined as follows:

$$(4.1) \quad a + b = \lim_{i \rightarrow \infty} (a^{p^i} b^{p^i})^{1/p^i}, \quad [a, b]_L = \lim_{i \rightarrow \infty} [a^{p^i}, b^{p^i}]^{1/p^{2i}}, \quad \forall a, b \in N,$$

where $[a, b] = a^{-1}b^{-1}ab$ is the commutator defined in the group N . We write $L_{\mathbb{Q}_p}(N) = \mathbf{log}(N) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ and we refer to this Lie \mathbb{Q}_p -algebra as the Lie algebra associated to N .

Let P be a pro- p group of finite rank and N an open normal uniform subgroup of P . Then conjugation by P provides **log**(N) with the structure of a P -module,

via the adjoint representation. For $g \in P$ we denote by $ad(g) \in \text{End}_{\mathbb{Z}_p}(\mathbf{log}(N))$ the endomorphism corresponding to the conjugation action by g :

$$ad(g)(n) = g^{-1}ng, \forall n \in N.$$

By a slight abuse of notation, we denote also by $ad(g)$ the extension of $ad(g)$ to $L_{\mathbb{Q}_p}(N)$. The Lie algebra $L_{\mathbb{Q}_p}(N)$, regarded as a P -module via the action of P on it by conjugation, does not depend on the choice of N and it is an invariant of P , called the Lie algebra $\mathcal{L}(P)$ associated to P . If we consider only the Lie structure on $\mathcal{L}(P)$, then $\mathcal{L}(P)$ is a virtual invariant of P (i.e. the Lie algebra associated to an open subgroup of P is isomorphic to $\mathcal{L}(P)$).

Lemma 4.3. *Let P be a pro- p group of finite rank and N a normal uniform subgroup of P . For each $k \geq 0$, we put $N_k = N^{p^k}$. Let $i, j \in \mathbb{N}$ be such that $i \leq j \leq 2i + 1$. Then N_i/N_j is abelian and*

$$N_i/N_j \cong \mathbf{log}(N)/p^{j-i}\mathbf{log}(N)$$

as P -modules (P acts on N_i/N_j by conjugation and on $\mathbf{log}(N)/p^{j-i}\mathbf{log}(N)$ via the adjoint map).

Proof. The lemma is a consequence of the definition of sum in (4.1). □

The following lemma provides information about some real elements of pro-2 groups of finite rank. If N is a finite-index normal subgroup of a profinite group P , then $\text{Irr}(P|N)$ denotes the set of irreducible characters of G whose restriction to N is non-trivial.

Lemma 4.4. *Let P be a pro-2 group of finite rank and N a normal uniform subgroup of P . Then the following statements are equivalent:*

- (1) *there are $g \in P$ and $0 \neq l \in L_{\mathbb{Q}_2}(N)$ such that $ad(g)(l) = -l$;*
- (2) *there are $g \in P$ and $1 \neq n \in N$ such that $g^{-1}ng = n^{-1}$;*
- (3) *for infinitely many $t \in \mathbb{N}$ there are $g_t \in P$ and $\psi_t \in \text{Irr}(N_t/N_{2t}|N_{2t-2}/N_{2t})$ such that $\psi_t^{g_t} = \psi_t$.*

Proof. (1) and (2) are equivalent statements with different notation (of course, note that if -1 is an eigenvalue of $ad(g)$ in $L_{\mathbb{Q}_p}$, then it is also an eigenvalue of $ad(g)$ in $\mathbf{log}(N)$). Suppose (2) holds. Let $t \in \mathbb{N}$. The finite group N_t/N_{2t} is abelian of exponent 2^t . If t is large enough, by possibly taking a power of n instead of n , we can assume that nN_{2t} is an element of order 2^t such that $g^{-1}(nN_{2t})g = (nN_{2t})^{-1}$. By duality, there exists a character ψ of order 2^t of N_t/N_{2t} such that $\psi^g = \psi^{-1} = \bar{\psi}$. Since N_t/N_{2t-2} has exponent 2^{t-2} we have that ψ is non-trivial on N_{2t-2} .

Suppose now that (3) holds. Note that if $\psi_t \in \text{Irr}(N_t/N_{2t}|N_{2t-2}/N_{2t})$, then ψ_t has order at least 2^{t-1} . Then by duality, for infinitely many $t \in \mathbb{N}$ there exists $n_t N_{2t}$ in N_t/N_{2t} of order at least 2^{t-1} and $g_t \in P$ such that $g_t^{-1}(n_t N_{2t})g_t = (n_t N_{2t})^{-1}$. In particular, note that $n_t \in N_t \setminus N_{t+2}$. By Lemma 4.3, for any such t there exists $x_t \in \mathbf{log}(N) \setminus 4\mathbf{log}(N)$ such that

$$ad(g_t)(x_t) \equiv -x_t \pmod{2^t \mathbf{log}(N)}.$$

For any such t , let $X_t \subseteq P \times (\mathbf{log}(N) \setminus 4\mathbf{log}(N))$ be the set of elements (g, x) satisfying $ad(g)(x) \equiv -x \pmod{2^t \mathbf{log}(N)}$, so X_t is non-empty. Note that each X_t is closed, and therefore compact. Now $X_{t_1} \subseteq X_{t_2}$ if $t_1 \geq t_2$, and $\{X_t\}_t$ is an inverse system with the inclusion maps. The inverse limit of this inverse system is non-empty (by Theorem 1.4 of [3]), so there are $g \in P$ and $x \in \mathbf{log}(N) \setminus 4\mathbf{log}(N)$

such that for infinitely many t , $ad(g)(x) \equiv -x \pmod{2^t \log(N)}$. Since $\{2^t \log(N)\}$ constitutes a base of open neighbourhoods of the identity element of $\log(N)$, we have that $ad(g)(x) = -x$, as wanted. \square

As a consequence of the above lemma, we obtain that pro-2 groups of finite rank with a finite number of real irreducible characters admit the following equivalent characterizations.

Proposition 4.5. *Let P be a pro-2 group of finite rank. Then the following statements are equivalent:*

- (1) P is \mathbb{R} -finite;
- (2) any real element of P belongs to $rad_f(P)$;
- (3) P has a finite number of real conjugacy classes;
- (4) any real element of P has finite order;
- (5) -1 is not an eigenvalue of $ad(g)$ for any $g \in P$.

Proof. The fact that (1) implies (3) is already proved in Lemma 3.1 (4). It is evident that (2) implies (3), and (3) implies (4) by the arguments in the proof of Lemma 3.1. If we assume (1) and (4), then (2) follows by Lemma 4.2(3). Hence we have that (1) implies (2). Now (5) follows from (4), because if N is an open normal uniform subgroup of P and -1 is an eigenvalue of $ad(g)$ in its action on $L_{\mathbb{Q}_p}(N)$, then by Lemma 4.4 N contains a non-trivial real element of P , which would have infinite order because N is torsion-free.

Let us prove that (1) follows from (5). By way of contradiction assume that P has infinitely many real irreducible characters $\{\lambda_i\}_{i \in \mathbb{N}}$. As above, suppose that N is an open normal uniform subgroup of P . Let t_i be such that $\ker \lambda_i \geq N_{2t_i}$ but $\ker \lambda_i \not\geq N_{2t_i-2}$ and let $\psi_i \in \text{Irr}(N_{t_i}/N_{2t_i} | N_{2t_i-2}/N_{2t_i})$ be an irreducible component of the restriction of λ_i on N_{t_i} . Since λ_i is real, there exists $g_i \in P$ such that $\psi_i^{g_i} = \bar{\psi}_i$. Hence, by the implication from (3) to (1) in Lemma 4.4, -1 is an eigenvalue of $ad(g)$ for some $g \in P$, a contradiction. \square

Corollary 4.6. *Let P be a \mathbb{R} -finite pro-2 group. Then any closed subgroup of P is also \mathbb{R} -finite.*

Proof. Let T be a closed subgroup of P . Since P is \mathbb{R} -finite, P is of finite rank, by Lemma 4.2(1), and so T is also of finite rank. A real element of T is also real in P . Since all the real elements of P are of finite order, all the real elements of T are of finite order. Thus, the previous proposition implies that T is \mathbb{R} -finite. \square

In the next lemma we analyze some real elements of quotients of a semidirect product $P \rtimes \langle \phi \rangle$, where ϕ is an automorphism of P of order 2.

Lemma 4.7. *Let P be a pro-2 group of finite rank, N a normal open uniform subgroup of P and ϕ an automorphism of P of order 2 that fixes N . Then for any $s > t \geq 2$ and for any $n \in N_t$ such that $\phi(n)N_s = n^{-1}N_s$, there exists $m \in N_{t-1}$ such that $nN_{s-1} = \phi(m^{-1})mN_{s-1}$.*

Proof. We prove the lemma by induction on $s - t$. If $s = t + 1$ we can take $m = 1$. Consider the case $s = t + 2$. Note that N_{t-1}/N_{t+2} is abelian. Let $m \in N_{t-1}$ be such that $m^2 = n$. Then

$$(\phi(m^{-1})m)^2 N_{t+2} = \phi(n^{-1})n N_{t+2} = n^2 N_{t+2}.$$

Hence $nN_{t+1} = \phi(m^{-1})mN_{t+1}$.

Now assume $s > t + 2$. Then by induction, there exist $l \in N_{t-1}$ such that $nN_{s-2} = \phi(l^{-1})lN_{s-2}$. Let $k = nl^{-1}\phi(l)$. Since $N_{s-2}/N_s \subseteq Z(N/N_s)$, nN_s commutes with $\phi(l^{-1})lN_s$ and so

$$\phi(k)kN_s = \phi(n)\phi(l^{-1})lnl^{-1}\phi(l)N_s = N_s.$$

Since $k \in N_{s-2}$, by the case $s - t = 2$, there exists $v \in N_{s-3}$ such that $kN_{s-1} = \phi(v^{-1})vN_{s-1}$. Hence, since $N_{s-3}/N_{s-1} \leq Z(N/N_{s-1})$,

$$nN_{s-1} = k\phi(l^{-1})lN_{s-1} = \phi(v^{-1})v\phi(l^{-1})lN_{s-1} = \phi((lv)^{-1})lvN_{s-1}.$$

□

5. JUST INFINITE QUOTIENTS OF PRO-2 GROUPS WITH ODD NUMBER OF REAL CHARACTERS

In this section we start the study of infinite pro-2 groups having an odd number of real irreducible characters. Recall that a profinite group is called **just infinite** if it is infinite and it does not have proper infinite continuous quotients. Every infinite finitely generated pro- p group has at least one just infinite quotient. It turns out that every just infinite quotient of a pro-2 group with an odd number of real irreducible characters also has an odd number of real irreducible characters.

Theorem 5.1. *Let P be an infinite pro-2 group with a (finite) odd number of real irreducible characters. Then $P/\text{rad}_f(P)$ has also an odd number of real irreducible characters.*

Proof. Let N be a normal open uniform subgroup of P such that $\text{Irr}_r(P) \subseteq \text{Irr}(P/N)$ (by Lemma 4.2). Suppose that $K = \text{rad}_f(P)$, and write $\bar{A} = AK/K$ for each $A \subseteq P$ (for simplicity, we denote the images of N and N_t in \bar{P} just by N and N_t respectively). Also, for each $x \in K$, let $T_x = C_P(x)$. Since N and K commute, we have that $N \leq T_x$. By Lemma 4.2(3), \bar{P} , and so \bar{T}_x , is torsion free. By Corollary 4.6, \bar{T}_x is also \mathbb{R} -finite, and thus \bar{T}_x does not contain non-trivial real elements, by Proposition 4.5(2). Again by Proposition 4.5(2) and by Lemma 3.1(2), there exists $k_x \in \mathbb{N}$ such that for every $t \geq k_x$, the real elements of P/N_t are in NK/N_t , and the real elements of \bar{T}_x/N_t lie in N/N_t .

Let $t \geq \max_{x \in K} k_x$. Since $k(P/N_t)$ is odd, there exists $x \in K$ such that $k_P(Cl_P(x)N/N_t)$ is odd. Put $T = T_x$. Hence

$$k_T(N/N_t) = k_T(xN/N_t) = k_P(Cl_P(x)N/N_t),$$

since that map sending each T -conjugacy class in xN/N_t into the P -conjugacy class in $Cl_P(x)N/N_t$ which contains it is a bijection, because $N \cap K = 1$. In particular $k_T(N/N_t)$ is odd. Now inversion defines an action on N/N_t of order at most 2, so $k_T(N/N_t) \equiv r_T(N/N_t) \pmod{2}$. Thus \bar{T}/N_t has an odd number of real irreducible characters, by the choice of t . By enlarging t if necessary, we can assume that $\text{Irr}_r(\bar{T}) \subseteq \text{Irr}_r(\bar{T}/N_t)$, so \bar{T} has an odd number of real irreducible characters. Since there are no real elements in $\bar{P} \setminus \bar{T}$, Corollary 3.2 implies that $\bar{P} = \bar{T}$. □

Corollary 5.2. *Let P be an infinite pro-2 group with odd number of real irreducible characters. Then any just infinite quotient of P has an odd number of real characters.*

Proof. Let N be a normal open uniform subgroup of P such that $\text{Irr}_r(P) \subseteq \text{Irr}_r(P/N)$ (Lemma 4.2). Let M be a closed normal subgroup of P such that P/M is just infinite. Then $P/(N \cap M)$ has an odd number of real irreducible characters. Note that $M/N \cap M = \text{rad}_f(P/N \cap M)$, so P/M has also an odd number of real irreducible characters by the above result. \square

Corollary 5.3. *Let P be an infinite pro-2 group with odd number of real irreducible characters. Then P is not solvable.*

Proof. Let \bar{P} be a just infinite quotient of P . Since \bar{P} is just infinite, $\text{rad}_f(\bar{P}) = \{1\}$. Now, using that \bar{P} is \mathbb{R} -finite, we obtain that \bar{P} is torsion-free. Thus, if \bar{P} is solvable, it is isomorphic to \mathbb{Z}_2 (the only solvable torsion-free just infinite pro-2 group). However, \mathbb{Z}_2 has only 2 real irreducible characters. This is a contradiction, because \bar{P} should have an odd number of real irreducible characters by the previous corollary. \square

6. TORSION FREE PRO-2 GROUPS WITH ODD NUMBER OF REAL IRREDUCIBLE CHARACTERS

In this section we show that a torsion free pro-2 group P with an odd number of real irreducible characters and such that P can be embedded non-trivially as a subgroup of index 2 in another pro-2 group, contains a proper pro-2 subgroup with an odd number of real irreducible characters. Furthermore, the proper pro-2 subgroup of P that we obtain has at most as many real irreducible characters as P . This is the main step in the proof of Theorem A and it will be used in inductive arguments.

Theorem 6.1. *Let P be a torsion free subgroup of a pro-2 group Q of index 2. Assume that P has an odd number of real irreducible characters. Then there exists an element $x \in Q \setminus P$ such that $C_P(x)$ has an odd number of real irreducible characters and $|\text{Irr}_r(C_P(x))| \leq |\text{Irr}_r(P)|$.*

Proof. Since P has an odd number of real irreducible characters and P has index 2 in Q , by Corollary 3.2 there exists a real element a of Q in $Q \setminus P$. Then a^2 lies in P and it is real in P , because a^2 is real in Q and it is centralized by a . Since P is \mathbb{R} -finite, Proposition 4.5 implies that a^2 has finite order, and thus a has order 2 because P is torsion free. In particular, note that every real element of Q contained in aP is an involution

Observe that by Lemma 4.2(1), P has finite rank. Let N be a normal uniform open subgroup of Q contained in P . Let S be the set of elements of order 2 in Q . By Lemma 3.1(2) applied to the normal closed subset $S = aP$ of Q , we have that for large k all the real elements of aP/N_k are in SN_2/N_k . Now, by Lemma 4.1, there are only finitely many Q -conjugacy classes in S , so let $\{a_1, \dots, a_s\}$ be a set of representatives of these conjugacy classes.

We claim that $\{a_1N_2, \dots, a_sN_2\}$ lie in different conjugacy classes in Q/N_2 , and thus the Q -orbits of the subsets $a_1N_2/N_k, \dots, a_sN_2/N_k$ in Q/N_k are mutually disjoint. Indeed, note that if $(a_iN_2)^g = a_jN_2$ for some $g \in Q$ and $1 \leq i, j \leq s$, then $n = a_ja_i^g$ lies in N_2 . Hence

$$n^{a_j}n = (a_jn)^2 = (a_i^g)^2 = 1.$$

By Lemma 4.7, for each $s > 2$ there exists $m \in N_1$ such that $nN_{s-1} = (m^{-1})^{a_j}mN_{s-1}$. Hence

$$a_i^g N_{s-1} = a_j n N_{s-1} = a_j^m N_{s-1},$$

and we deduce that a_j is conjugate to a_i in Q because the subgroups N_s constitute a base of neighbourhoods of the identity. Thus $i = j$, as wanted.

By the previous paragraph, we have

$$(6.1) \quad r_Q(aP/N_k) = \sum_{i=1}^s r_Q(a_i N_2/N_k),$$

for k large enough. Since P has index 2 in Q , by Lemma 2.2 $r_Q(aP/N_k)$ is congruent to $r(P/N_k)$ modulo 2, for $k \in \mathbb{N}$. If we take k large enough, then $r(P/N_k) = |\text{Irr}_r(P)|$ by Lemma 4.2(2), so there exists i such that $r_Q(a_i N_2/N_k)$ is odd.

Next we work to prove the main step in the proof, namely that for any element $a \in Q \setminus P$ of order 2,

$$(6.2) \quad |\text{Irr}_r(C_P(a))| = r_Q(aN_2/N_k),$$

if k is large enough. Of course, this will complete the proof of the first part of the theorem. In order to prove the second part of the result, it is enough to show that $|\text{Irr}_r(C_P(a))| \leq |\text{Irr}_r(P)|$ for all such a . It is clear that (6.2) implies that $|\text{Irr}_r(C_P(a))| \leq r_Q(aP/N_k)$, and thus if k is large enough, then it follows from Proposition 2.6 that $|\text{Irr}_r(C_P(a))| \leq |\text{Irr}_r(P)|$. Therefore proving (6.2) will complete the proof of the theorem.

We fix an element $a \in Q \setminus P$ of order 2 for the rest of the proof. By Corollary 4.6, $C_P(a)$ is \mathbb{R} -finite. Let

$$r = \max\{|\text{Irr}_r(P)|, |\text{Irr}_r(C_P(a))|\}.$$

The following follows easily from the choice of r :

Claim 1. *For $k \geq r$ large enough, suppose that M is an open normal subgroup of P (respectively of $C_P(a)$) contained in N_k (resp. in $C_{N_k}(a)$). Then all real elements of P/M (resp. of $C_P(a)/M$) are contained in N_{k-r+1}/M (resp. in $C_{N_{k-r+1}}(a)/M$).*

Proof. By Lemma 2.4, $r(P/M) \leq r$. Since P is \mathbb{R} -finite and torsion-free, P has no non-trivial real elements by Proposition 4.5. Then by Lemma 3.1 there exists an open normal subgroup L of P contained in N , such that all real elements of P/L lie in N/L . Now let k be large enough so that $N_k \leq L$. Suppose that $M \leq N_k$, so the real elements of P/M lie in N/M . Then if yM is a real element of P/M not contained in N_{k-r+1}/M , the powers of yM provide representatives of at least $r+1$ distinct real classes in P/M , which is a contradiction. The same argument works for $C_P(a)$. \square

Claim 2. *Let $k \geq r+2$ be large enough. Then $r_Q(aN_2/N_k) = r_P(aN_{k-r}/N_k)$.*

Proof. Since P has index 2 in Q , it is clear that Q -conjugate elements in $(Q \setminus P)N_k/N_k$ are P -conjugate. Thus

$$r_Q(aN_2/N_k) = r_P(aN_2/N_k).$$

Let $y = an \in aN_2$ be such that yN_k is a P -real element of Q/N_k . Then $y^2N_k = n^a n N_k$ is real in P/N_k . Hence $n^a n \in N_{k-r+1}$, by Claim 1. By Lemma 4.7 (ϕ is the conjugation by a), there exists $m \in N/N_k$ such that $anN_{k-r} = a^m N_{k-r}$, so any

P -conjugacy class of an element $yN_k \in aN_2/N_k$ which is inverted by P intersects with aN_{k-r} . Therefore:

$$r_P(aN_2/N_k) = r_P(aN_{k-r}/N_k),$$

as wanted. \square

Observe that it is clear from the previous claim that if $N_{k-r} \leq H \leq N_2$, then

$$(6.3) \quad r_Q(aN_2/N_k) = r_P(aH/N_k).$$

Claim 3. *Let k be sufficiently large. Then the following holds:*

- (1) *The real elements of $C_P(a)/C_{N_{k-1}}(a)$ are in $C_N(a)/C_{N_{k-1}}(a)$;*
- (2) *$\text{Irr}_r(C_P(a)) \subseteq \text{Irr}(C_P(a)/C_{N_{k-1}}(a))$;*
- (3) *$C_P(aN_k) \leq C_P(a)N_{r+2}$;*
- (4) *$C_{N_k}(aN_{2k}) \leq C_{N_k}(a)N_{k+r+2}$.*

Proof. Since P is \mathbb{R} -finite and torsion free, P has no non-trivial real elements. Thus Lemma 3.1(2) (with P , \mathcal{S} and N replaced by $C_P(a)$, $C_P(a)$ and $C_N(a)$, respectively) implies (1). Also, Lemma 4.2(2), implies (2).

Now we prove the third statement. If there are infinitely many $k \geq r+2$ such that $C_P(aN_k) \not\leq C_P(a)N_{r+2}$, then for each such k we can find an element $x_k \in C_P(aN_k) \setminus C_P(a)N_{r+2}$. Since P is compact, some subsequence $\{x_{k_i}\}$ of $\{x_k\}$ has a limit x that belongs to $\cap_{i=1}^{\infty} C_P(aN_{k_i}) = C_P(a)$. However $P \setminus C_P(a)N_{r+2}$ is closed, whence $x \notin C_P(a) \leq C_P(a)N_{r+2}$, a contradiction. Thus, there exist only finitely many k such that $C_P(aN_k) \not\leq C_P(a)N_{r+2}$. This gives the third statement.

The last statement can be proved similarly, once one notes that it is equivalent to the following claim:

$$C_{\log(N)}(a + 2^k \log(N)) \leq C_{\log(N)}(a) + 2^{r+2} \log(N).$$

\square

Claim 4. *Let k be large enough and suppose that $N_{k-r-1} \leq H \leq N_{k-r-2}$. Then:*

$$r_Q(aN_2/N_k) = r_{C_P(a)N_{r+2}}(aH/N_k).$$

Proof. Note that if $ah_1N_k, ah_2N_k \in aH/N_k$ are conjugate via $g \in P$, then $(aN_{k-r-2})^g = aN_{k-r-2}$, so $g \in C_P(aN_{k-r-2})$ and thus

$$(6.4) \quad r_P(aH/N_k) = r_{C_P(aN_{k-r-2})}(aH/N_k).$$

Since $C_P(aN_{k-r-2}) \leq C_P(a)N_{r+2}$ by Claim 3(3), we obtain from (6.4) that:

$$(6.5) \quad r_{C_P(aN_{k-r-2})}(aH/N_k) = r_{C_P(a)N_{r+2}}(aH/N_k).$$

Now, if we put together (6.3), (6.4) and (6.5), we obtain the claim. \square

For k large enough we define

$$A = C_{N_{k-r-2}}(a),$$

and

$$J = \{z^a z^{-1} N_k \in Q/N_k : z \in N_{r+2}\} \cap N_{k-r-2}/N_k.$$

We observe that J is an abelian subgroup of Q/N_k . Indeed, if $z_i^a z_i^{-1} N_k \in J$ with $z_i \in N_{r+2}$ and $i = 1, 2$, then

$$z_1^a z_1^{-1} z_2^a z_2^{-1} N_k = z_1^a z_2^a z_2^{-1} z_1^{-1} N_k = (z_1 z_2)^a (z_1 z_2)^{-1} N_k,$$

because $N_{k-r-2}/N_k \leq Z(N_{r+2}/N_k)$. So let $N_k \leq B$ be the subgroup of Q such that $B/N_k = J$. Since $C_P(a)$ normalizes B , we have that AB is a subgroup of N_{k-r-2} , and also $C_P(a)$ acts on the set of left cosets of B in AB .

Claim 5. *Let k be large enough. Then N_{k-r-1} is contained in AB .*

Proof. Let $y \in N_{k-r-2}$. Then $y^2 = (yy^a)((y^{-1})^a y)$. Note that

$$yy^a \in C_{N_{k-r-2}}(aN_{2k-2r-4}),$$

and thus $yy^a \in AN_k$ by Claim 3(4). Thus y^2 lies in AB . Therefore, $N_{k-r-1}/N_k = (N_{k-r-2})^2/N_k \leq AB/N_k$. \square

Note that in particular we have that

$$N_{k-r-1} \leq AB \leq N_{k-r-2}.$$

Thus, by Claim 4 if k is large enough then

$$(6.6) \quad r_Q(aN_2/N_k) = r_{C_P(a)N_{r+2}}(aAB/N_k).$$

The aim of introducing the subgroups A and B is to compare the action by conjugation of Q with that of $C_P(a)$. We have the following:

Claim 6. *Let $h_1, h_2 \in AB$. Then there exists $g \in C_P(a)N_{r+2}$ such that $(ah_1)^g N_k = ah_2 N_k$ if and only if there exists $c \in C_P(a)$ such that $(h_1)^c B = h_2 B$.*

Proof. Firstly assume that

$$(h_1)^c B = h_2 B \text{ for some } c \in C_P(a).$$

Hence there exists $b \in B$ such that $(h_1)^c = h_2 b$. Let $n \in N_{r+2}$ be such that $a^n N_k = ab^{-1} N_k$. Hence

$$(ah_1)^{cn} N_k = (a(h_1)^c)^n N_k = a^n h_2 b N_k = ah_2 N_k,$$

where we are using that $N_{k-r-2}/N_k \leq Z(N_{r+2}/N_k)$.

Secondly, we assume that

$$(ah_1)^g N_k = ah_2 N_k \text{ for some } g \in C_P(a)N_{r+2}.$$

Write $g = cm$, where $c \in C_P(a)$ and $m \in N_{r+2}$. Hence

$$ah_2 N_k = (ah_1 N_k)^g = a^m h_1^c N_k,$$

where again the last equality holds because N_{k-r-2}/N_k is centralized by N_{r+2} . Thus

$$aa^m N_k \subseteq B,$$

and so

$$h_2 \equiv h_1^c \pmod{B}.$$

\square

Claim 7. *Let k be large enough. Then $r_{C_P(a)N_{r+2}}(aAB/N_k) = r_{C_P(a)}(AB/B)$.*

Proof. Let $n \in AB$. Since $(an)^{-1} = n^{-1}a = an^{-1}[n^{-1}, a]$ and $[n^{-1}, a] \in B$, by Claim 6 we have that anN_k is real in $C_P(a)N_{r+2}/N_k$ if and only if there exists $c \in C_P(a)$ such that $n^c \equiv n^{-1} \pmod{B}$. Thus,

$$r_{C_P(a)N_{r+2}}(aAB/N_k) = r_{C_P(a)}(AB/B).$$

\square

In order to finish the proof, we need one more observation:

Claim 8. *Let k be large enough. Then*

$$r_{C_P(a)}(AB/B) = |\text{Irr}_r(C_P(a))|.$$

Proof. Observe that

$$(z^a z^{-1})^a = z(z^{-1})^a = (z^a z^{-1})^{-1},$$

for any $z \in N_{r+2}$. In particular, $(A \cap B)N_k/N_k$ has exponent 2, and so $M = A \cap B \subseteq C_{N_{k-1}}(a)$. By Claim 1, all real elements of $C_P(a)/M$ are in

$$C_{N_{k-r}}(a)/M \leq A/A \cap B \cong AB/B.$$

By Claim 3, we have that $\text{Irr}_r(C_P(a)) = \text{Irr}_r(C_P(a)/M)$ and the claim follows. \square

Now, if we put together (6.6), Claim 7 and the previous claim we obtain that

$$|\text{Irr}_r(C_P(a))| = r_Q(aN_2/N_k)$$

holds for any k large enough, as wanted. The proof is complete. \square

7. JUST INFINITE PRO-2 GROUPS WITH ODD NUMBER OF REAL IRREDUCIBLE CHARACTERS

Observe that by Corollary 5.2 and Corollary 5.3, in order to understand pro-2 groups with odd number of real irreducible characters one has to consider non-solvable just infinite pro-2 groups of finite rank. Also, Theorem 6.1 indicates that we have to look at “minimal” examples of such groups. As it will follow from the results in this section, these groups are Sylow pro-2 groups of $\text{Aut}(\mathfrak{sl}_1(D))$, where D is some finite-dimensional division algebra over \mathbb{Q}_2 .

Just infinite pro- p groups of finite rank are well understood. We refer to the book [8] for detailed information on these groups, including their classification. Let P be a non-solvable just infinite pro- p group of finite rank. Then it is known (see [8, Proposition III.6]) that $\mathcal{L}(P)$ is a semi-simple Lie \mathbb{Q}_p -algebra, and all summands appearing in the decomposition of $\mathcal{L}(P)$ as a sum of simple Lie algebras are isomorphic. Since P is just infinite, we have that $\ker ad = \{1\}$. In fact, $ad(P)$ is an open subgroup in $\text{Aut}(\mathcal{L}(P))$ isomorphic to P . By [8, Lemma III.16], $\text{Aut}(\mathcal{L}(P))$ contains a Sylow pro- p subgroup, that is a maximal pro- p subgroup, and the Sylow pro- p subgroups of $\text{Aut}(\mathcal{L}(P))$ are all conjugate.

Let \mathcal{L} be a simple finite-dimensional \mathbb{Q}_2 -algebra. Then the centroid K of \mathcal{L} is defined as

$$\text{End}_{\mathcal{L}}(\mathcal{L}) = \{\phi \in \text{End}_{\mathbb{Q}_2}(\mathcal{L}) : [\phi(l), m] = \phi([l, m]) \text{ for every } l, m \in \mathcal{L}\}.$$

It can be shown that K is in fact a finite extension field of \mathbb{Q}_2 , and \mathcal{L} may be regarded in a natural way as a Lie K -algebra, denoted by a slight abuse of notation \mathcal{L} as well. The K -algebra \mathcal{L} is absolutely simple, i.e. for any field extension F/K the Lie F -algebra $\mathcal{L} \otimes_K F$ is simple (see Chapter X of [7]).

We shall describe a standard construction of an absolutely simple algebraic group $\mathbf{G} = \mathbf{G}_{\mathcal{L}}$ defined over K such that $\mathbf{G}(K) \cong \text{Aut}_K(\mathcal{L})$ and moreover, if E is an

extension of K , then $\mathbf{G}(E) \cong \text{Aut}_E(\mathcal{L} \otimes_K E)$. This is done in the following way. Fix a basis $B = \{l_1, \dots, l_n\}$ of \mathcal{L} over K and define $a_{ij}^k \in K$ as follows

$$[l_i, l_j]_L = \sum_{k=1}^n a_{ij}^k l_k.$$

Let ϕ be an automorphism of the Lie K -algebra \mathcal{L} and let $X = (x_{ij}) \in \text{GL}_n(K)$ be such that

$$\phi(l_i) = \sum_{j=1}^n x_{ij} l_j.$$

Then we obtain that

$$(7.1) \quad \sum_{u=1}^n a_{ij}^u x_{uk} = \sum_{s,t=1}^n a_{st}^k x_{is} x_{jt}, \text{ for all } 1 \leq i, j, k \leq n.$$

Then we define $\mathbf{G} = \mathbf{G}_{\mathcal{L}}$ to be the algebraic subvariety of \mathbf{GL}_n defined by the equations (7.1). In fact, one can easily check that \mathbf{G} is an algebraic subgroup of \mathbf{GL}_n and $\mathbf{G}(E) \cong \text{Aut}_E(\mathcal{L} \otimes_K E)$.

Denote by \mathbf{G}^o the connected component of the identity of \mathbf{G} . Note that \mathbf{G}^o is also defined over K (see [4, 34.2]). The algebraic group \mathbf{G}^o is of adjoint type (see [4, 31.1]). Denote by $\tilde{\mathbf{G}}^o$ the simply connected cover of \mathbf{G}^o (see [10, Theorem 2.6]). By [10, Proposition 2.10], there exists a universal covering $\pi : \tilde{\mathbf{G}}^o \rightarrow \mathbf{G}^o$ defined over K . In particular $\tilde{\mathbf{G}}^o$ can be defined over K .

Since \mathbf{G} is a K -group, its Lie algebra (see [4, 9.1]) has a K -structure (see [4, 34.2]). Arguing as in the proof of [4, Corollary 13.2], we obtain that the K -points of the Lie algebra of \mathbf{G} is isomorphic to the algebra $\mathfrak{Der}_K(\mathcal{L})$ of K -derivations of \mathcal{L} . Since \mathcal{L} is simple, $\mathfrak{Der}_K(\mathcal{L}) \simeq \mathcal{L}$ (see [4, 14.1]). Thus, the K -points of the Lie algebra of \mathbf{G} are isomorphic to \mathcal{L} . In particular, \mathbf{G} is absolutely simple.

Now, we consider a particular case of the previous situation. If K is a field, we say that a division algebra D is K -central if $Z(D) \cong K$ and D has finite dimension over K . Suppose that K is a finite extension of \mathbb{Q}_2 , and let D be a finite-dimensional K -central division algebra. Suppose that E is a splitting field for D , so by definition there exists an isomorphism of E -algebras $\varphi : D \otimes_K E \simeq M_d(E)$, where d is the index of D (recall that E can be taken to be any field containing a maximal subfield of D , see Theorem 7.15 of [11] and the discussion before it). For each element $x \in D$ we denote its **reduced trace** by way of

$$\text{trd}(x) = \text{tr}(\varphi(x \otimes_K 1_E)).$$

Let $\mathfrak{sl}_1(D)$ be the elements of D of reduced trace 0. Then $\mathfrak{sl}_1(D)$ is a simple Lie \mathbb{Q}_2 -algebra with Lie bracket defined by $[x, y]_L = xy - yx$. One can show that in fact the algebraic group $\mathbf{G}_{\mathfrak{sl}_1(D)}$ is already connected. Let us describe its simply connected cover.

The **reduced norm** is the map given by $\text{Nrd}(x) = \det(\varphi(x \otimes_K 1))$, for all $x \in D$. It follows from the definition that Nrd is a multiplicative map. Also, the reduced norm is independent of the choice of E and φ , and it takes values in K (see Theorem 9.3 and p. 116 of [11]).

It is well-known that $\text{Nrd}(x)$ is given by a homogeneous polynomial of degree d with coefficients in K , in the coordinates of $x \in D$ with respect to an arbitrary fixed basis for D over K (see p. 27 of [10]). Next we define, following 2.3.1 in [10], an algebraic K -group $\mathbf{SL}_1(D)$ whose group of K -rational points is $\text{SL}_1(D) =$

$\{x \in D^* : \text{Nrd}(x) = 1\}$. For $x \in D$, let r_x be the K -linear map in D induced by right multiplication by x . The algebra representation $\rho : D \rightarrow M_{d^2}(K)$ sending each $x \in D$ to the matrix $\rho(x)$ of r_x with respect to a fixed K -basis for D is called the **regular representation** of D . Observe that the K -linear subspace $\rho(D)$ of $M_{d^2}(K)$ is the set of common zeros of a finite number of linear polynomials f_1, \dots, f_t with coefficients in K , in the coordinates of the matrices with respect to the canonical basis of $M_{d^2}(K)$. There exists a polynomial f with coefficients in K such that if $\rho(x) = (k_{ij}) \in M_{d^2}(K)$, then

$$f(k_{11}, \dots, k_{1d^2}, k_{21}, \dots, k_{d^2d^2}) = \text{Nrd}(x),$$

for all $x \in D$. We define $\mathbf{SL}_1(D)$ to be the algebraic subvariety of \mathbf{GL}_{d^2} defined by the equations $f_1 = \dots = f_t = f - 1 = 0$.

Now let Ω be an algebraic closure of K containing E . Observe that the vanishing set of f_1, \dots, f_t in $M_{d^2}(\Omega)$ is isomorphic as an Ω -algebra to $D \otimes_K \Omega \cong M_d(\Omega)$. Thus, if $b = (b_{ij}) \in M_{d^2}(\Omega)$ annihilates all polynomials $f - 1, f_1, \dots, f_t$, then b may be regarded as a point in $M_d(\Omega)$, and as such it has determinant equal to 1, because $f(b) = 1$. It then follows that $\mathbf{SL}_1(D)$ is an algebraic K -group Ω -isomorphic to \mathbf{SL}_d , and in particular it is simply connected.

Now, $\pi : \mathbf{SL}_1(D) \rightarrow \mathbf{G}_{\mathbf{SL}_1(D)}$ is defined in an obvious way because any point of $D \otimes_K \Omega$ induces by conjugation an automorphism of $\mathbf{SL}_1(D) \otimes_K \Omega$.

Theorem 7.1. *Let \mathcal{L} be a finite-dimensional semi-simple Lie \mathbb{Q}_2 -algebra all whose simple components are isomorphic. Assume that the Sylow pro-2 subgroups of $\text{Aut}(\mathcal{L})$ are torsion free. Then $\mathcal{L} \cong \mathbf{sl}_1(D)$ for some finite-dimensional division \mathbb{Q}_2 -algebra D .*

Proof. First observe that \mathcal{L} is simple. Indeed, if \mathcal{L} decomposes as a direct sum of more than one simple algebra, then the automorphism of \mathcal{L} that permutes two of the summands into which \mathcal{L} decomposes and acts as the identity on the rest of summands has order 2, which is a contradiction.

We use the notation introduced before the theorem. Let $\mathbf{G} = \mathbf{G}_{\mathcal{L}}$. Hence $\mathbf{G}(K) \cong \text{Aut}_K(\mathcal{L})$. First, let us show that \mathbf{G}° is K -isotropic, i.e. that the K -rank of \mathbf{G}° is zero (see [4, 34.5] for a definition of K -rank). Assume that the K -rank of \mathbf{G}° is not zero. Then \mathbf{G}° contains a K -split torus T of positive dimension n . Since the group $T(K)$ of K -points of T , which is isomorphic to $(K^*)^n$, contains an element of order 2 (because -1 is an element of K^* of order 2), we obtain a contradiction.

Since \mathbf{G}° is K -isotropic, $\tilde{\mathbf{G}}^\circ$ is also K -isotropic. Hence, by [9] (see also [10, Theorem 6.5]), $\tilde{\mathbf{G}}^\circ \cong \mathbf{SL}_1(D)$ for some K -central division algebra D . Thus, \mathcal{L} is isomorphic to $\mathbf{sl}_1(D)$. \square

8. REAL CHARACTERS OF SYLOW 2-PRO GROUPS OF $\text{PGL}_1(D)$

In this section we study the Sylow pro-2 subgroups of $\text{Aut}(\mathbf{sl}_1(D))$ having odd number of real irreducible characters, where D is a K -central division algebra over a finite degree extension K of \mathbb{Q}_2 .

Let K be a field. It is well-known (see [13]) that the isomorphism types of K -central division algebras are classified by the elements of the group $H^2(\text{Gal}(K_s/K), K_s^*)$, where K_s denotes the maximal algebraic separable extension of K . The situation when K is a finite extension of \mathbb{Q}_p is perfectly understood. From local class field theory we know that $H^2(\text{Gal}(K_s/K), K_s^*) = \mathbb{Q}/\mathbb{Z}$ in this case. In particular, this

implies that there are exactly $\phi(d)$ different (up to isomorphism) K -central division algebras of dimension d^2 over K and one can easily describe these algebras. We recommend the reader to look at [13] for details and proofs of the results that we present in the next paragraphs.

Let K be a finite extension of \mathbb{Q}_2 . Next we describe how to construct the different K -central division algebras of a given dimension d^2 . Denote by \mathcal{O}_K the ring of integers of K , which is a local ring, and let \mathfrak{m}_K be its maximal ideal. Then \mathfrak{m}_K is principal, and we choose a generator π_K of \mathfrak{m}_K . The residue class field $\mathcal{O}_K/\mathfrak{m}_K$ has order a power of 2, say q . Now, let w be a $(q^d - 1)$ th primitive root of unity and write $W = K(w)$. Then W/K is an unramified, cyclic Galois extension of degree d . The Galois group $\text{Gal}(W/K)$ is generated by the K -automorphism θ sending w to w^q , so the $\phi(d)$ distinct powers θ^r of θ , where r is coprime to d , are the generators of $\text{Gal}(W/K)$. Choose such a generator $\alpha = \theta^r$ sending w to w^{q^r} . Then the K -algebra D generated by W and an element π_D satisfying the following relations:

$$(8.1) \quad (\pi_D)^d = \pi_K \text{ and } (\pi_D)^{-1}v\pi_D = \alpha(v) \text{ for all } v \in W$$

is a K -central division algebra. The set $\{1, \pi_D, \dots, (\pi_D)^{d-1}\}$ is a basis of D over W , so D has dimension d^2 over K .

The following proposition describes the structure of $\text{Aut}_{\mathbb{Q}_2}(\mathfrak{sl}_1(D))$.

Proposition 8.1. *Let K be a finite extension of \mathbb{Q}_2 , D a K -central division algebra of dimension $\dim_K D = d^2 > 1$ and $\mathcal{L} = \mathfrak{sl}_1(D)$. Let $\Psi : \text{Aut}_{\mathbb{Q}_2}(D) \rightarrow \text{Aut}_{\mathbb{Q}_2}(\mathcal{L})$ be the restriction map. Then the map Ψ is an isomorphism.*

Proof. It is clear that any \mathbb{Q}_2 -automorphism of D fixes the Lie algebra \mathcal{L} and it induces an automorphism of \mathcal{L} . Thus, Ψ is well-defined. It is also clear that the map Ψ is a monomorphism. Let us show that Ψ is surjective. We divide the proof of this into several steps.

Claim 1. *Let ϕ be an element of $\text{Aut}_{\mathbb{Q}_2}(\mathcal{L})$. Then ϕ induces an automorphism of K (that we will denote also by ϕ) such that*

$$\phi(k)\phi(l) = \phi(kl) \text{ for every } k \in K \text{ and } l \in \mathcal{L}.$$

Proof. For every $k \in K$, let $\alpha_k : \mathcal{L} \rightarrow \mathcal{L}$ be a \mathbb{Q}_2 -linear map defined by means of

$$\alpha_k(l) = \phi(k\phi^{-1}(l)) \quad (l \in \mathcal{L}).$$

Then we see that for any $l, m \in \mathcal{L}$ we have that

$$\begin{aligned} [\alpha_k(l), m]_L &= [\phi(k\phi^{-1}(l)), m]_L = \phi([k\phi^{-1}(l), \phi^{-1}(m)]_L) = \\ &= \phi(k\phi^{-1}([l, m]_L)) = \alpha_k([l, m]_L). \end{aligned}$$

Hence α_k is an element of the centroid of \mathcal{L} , which is equal to K (since $\mathbf{G}_{\mathcal{L}}$ is an absolutely simple K -group, this follows from [7, Theorem 3 of Chapter X] by construction of $\mathbf{G}_{\mathcal{L}}$). Thus, α_k is represented by multiplication by a (uniquely defined) element of K . We denote this element of K by $\phi(k)$. One easily checks that $\phi : K \rightarrow K$ is an automorphism of K . \square

Claim 2. *Let ϕ be an element of $\text{Aut}_{\mathbb{Q}_2}(\mathcal{L})$. Then ϕ induces a \mathbb{Q}_2 -algebra automorphism of the enveloping K -algebra $U_K(\mathcal{L})$ of \mathcal{L} (that we will denote also by ϕ) that extends the action of ϕ on K and \mathcal{L} .*

Proof. Note that $U_K(\mathcal{L})$ can be defined as a \mathbb{Q}_2 -algebra generated by two \mathbb{Q}_2 -vector spaces K and \mathcal{L} with the following relations:

$$k \cdot l = l \cdot k = kl, \quad l \cdot m - m \cdot l = [l, m]_L \quad (k \in K, l, m \in \mathcal{L}).$$

In the previous relations \cdot is the multiplication in the algebra $U_K(\mathcal{L})$ and kl is considered as an element of the space \mathcal{L} . Since ϕ conserves these relations we can extend ϕ on $U_K(\mathcal{L})$. \square

Now, we will use an argument that appears in Lemma [8, XI.14]. Note that $\bar{K} \otimes_K D \cong \text{Mat}_d(\bar{K})$ and $\bar{K} \otimes_K U_K(\mathcal{L}) \cong U_{\bar{K}}(\mathfrak{sl}_d(\bar{K}))$.

Claim 3. *Let I_1 and I_2 be two ideals of $U_K(\mathcal{L})$. Then $I_1 \leq I_2$ if and only if $\bar{K}I_1 \leq \bar{K}I_2$.*

Proof. We have to prove only the “if” part. For this, observe that if $\bar{K}I_1 \leq \bar{K}I_2$, then

$$I_1 \leq U_K(\mathcal{L}) \cap \bar{K}I_2 = I_2.$$

\square

The embedding of \mathcal{L} into D induces a surjective homomorphism $U_K(\mathcal{L}) \rightarrow D$. We denote by I the kernel of this homomorphism. The Lie algebra \mathcal{L} can be also embedded into D^{op} (the opposite algebra of D) by sending $l \in \mathcal{L}$ to $-l \in D$. This embedding induces a surjective homomorphism $U_K(\mathcal{L}) \rightarrow D^{op}$. We denote by J the kernel of this homomorphism.

Claim 4. *Let $d \neq 2$. Then $D \not\cong D^{op}$ as \mathbb{Q}_2 -algebras. In particular, I and J are not equal.*

Proof. We have described the structure of D before this proposition, and we use the notation introduced there. The relevant parameters that determine D up to K -isomorphism are its center K , its index d and the number r ($1 \leq r \leq d$, $(r, d) = 1$). Another division K -algebra, with the same parameters as D , is K -isomorphic to D . Let us recall briefly how one can define r internally in terms of D .

The division algebra D contains a unique maximal compact subring $\mathcal{O}_D = \mathcal{O}_W[\pi_D]$ and $\pi_D \mathcal{O}_D$ is its maximal ideal. Recall that q is the size of the field $\mathcal{O}_K/\mathfrak{m}_K$ (and so, depends only on K). The group D^* contains a unique maximal compact subgroup \mathcal{O}_{D^*} which is known to be prosoluble of order $(q^d - 1)2^\infty$. Hence D^* contains a unique conjugacy class of subgroups of order $q^d - 1$ (which are, in fact, cyclic). Let $A = \langle a \rangle$ be one of such subgroups (for example, it can be $\langle w \rangle$). Take $g \in N_{D^*}(A) \cap (\pi_D \mathcal{O}_D \setminus \pi_D^2 \mathcal{O}_D)$. Then $a^g = a^{q^r}$ and r does not depend on the choices of a and g .

Let $\psi : D \rightarrow D^{op}$ be an isomorphism of \mathbb{Q}_2 -algebras. We want to show that D and D^{op} are isomorphic as K -algebras as well. The center of D^{op} is K and its index is equal to d . So we only have to analyze the parameter r corresponding to D^{op} .

Note that ψ is a topological isomorphism as well. Hence, $\phi(\mathcal{O}_D) = \mathcal{O}_{D^{op}}$ and $\psi(\pi_D \mathcal{O}_D) = \psi(\pi_D) \mathcal{O}_{D^{op}}$ is the maximal ideal of $\mathcal{O}_{D^{op}}$. Put $A = \langle \psi(w) \rangle$ and $g = \psi(\pi_D)$. Since $a^g = a^{q^r}$, we obtain from the previous discussion that D^{op} and D are isomorphic as K -algebras.

Let $[D] \in \text{Br}(K)$ denote the element of the Brauer group of K corresponding to the algebra D . Since K is a local field, the order of $[D]$ is d . Note that $[D]^{-1} = [D^{op}]$ and so if $D \cong D^{op}$, $d = 2$, a contradiction. \square

Claim 5. *Let Z be an ideal of K -algebra $U_K(\mathcal{L})$ of codimension d^2 such that $U_K(\mathcal{L})/Z$ is a central simple K -algebra. Then if $d = 2$, $Z = I$ and if $d > 2$ $Z = I$ or $Z = J$.*

Proof. Note that $\mathfrak{sl}_d(\bar{K})$ has a single irreducible module (up to isomorphism) of dimension 2 if $d = 2$ and exactly two irreducible modules of dimension d if $d > 2$.

Thus, if $d = 2$, $\bar{K}I$ is the only ideal of $U_{\bar{K}}(\mathfrak{sl}_d(\bar{K}))$ such that the quotient of $U_{\bar{K}}(\mathfrak{sl}_d(\bar{K}))$ by this ideal is isomorphic to $\text{Mat}_d(\bar{K})$. Claim 3 implies that $I = J$ is the only ideal of $U_K(\mathcal{L})$ such that the quotient of $U_K(\mathcal{L})$ by this ideal is a central simple K -algebra of dimension d^2 .

Assume now that $d > 2$. Since $I \neq J$, by Claim 3, $\bar{K}I \neq \bar{K}J$. Hence, if $d > 2$ there are exactly two ideals $\bar{K}I$ and $\bar{K}J$ of $U_{\bar{K}}(\mathfrak{sl}_d(\bar{K}))$ such that the quotient of $U_{\bar{K}}(\mathfrak{sl}_d(\bar{K}))$ by this ideal is isomorphic to $\text{Mat}_d(\bar{K})$, and so, there are exactly two ideals I and J of $U_K(\mathcal{L})$ such that the quotient of $U_K(\mathcal{L})$ by these ideals is a central simple K -algebra of dimension d^2 . \square

Claim 6. *Let ϕ be an element of $\text{Aut}_{\mathbb{Q}_2}(U_K(\mathcal{L}))$. Then $\phi(I) = I$.*

Proof. Note that $U_K(\mathcal{L})/\phi(I)$ is isomorphic to D (as \mathbb{Q}_2 -algebra). Thus, $\phi(I)$ is an ideal of K -algebra $U_K(\mathcal{L})$ of codimension d^2 and $U_K(\mathcal{L})/\phi(I)$ is a central simple K -algebra. Hence by the previous claim, $\phi(I) = I$ or $\phi(I) = J$. In the first case we are done.

Now, assume that $d > 2$ and $\phi(I) = J$. We want to show that it cannot happen. If this happens, then ϕ induces an \mathbb{Q}_2 -isomorphism between $U_K(\mathcal{L})/I \cong D$ and $U_K(\mathcal{L})/J \cong D^{op}$, but this is impossible by Claim 4. \square

Now, we are ready to finish the proof of the proposition. Let ϕ be an element of $\text{Aut}_{\mathbb{Q}_2}(\mathcal{L})$. Then by Claim 2, ϕ extends to a \mathbb{Q}_2 -automorphism of $U_K(\mathcal{L})$. By Claim 6, $\phi(I) = I$. Hence ϕ induces a \mathbb{Q}_2 -automorphism of $U_K(\mathcal{L})/I \cong D$ which extends the action of ϕ on \mathcal{L} . This finishes the proof of the proposition. \square

We write D^* for the multiplicative group of non-zero elements of D and $\text{PGL}_1(D) = D^*/Z(D^*)$. Recall that by the Skolem-Noether Theorem, $\text{Aut}_K(D) \cong \text{PGL}_1(D)$.

Now let us describe the structure of $\text{PGL}_1(D)$. Let $\mathcal{O}_D = \mathcal{O}_W[\pi_D]$ and let U_D be its unit group. Note that $\mathbf{m}_D = \mathcal{O}_D\pi_D = \pi_D\mathcal{O}_D = (\pi_D)$ is the unique maximal ideal of \mathcal{O}_D , and $\mathcal{O}_D/\mathbf{m}_D \cong \mathcal{O}_W/\mathbf{m}_W \cong \mathbb{F}_{q^d}$. Define the following subgroups of $\text{PGL}_1(D)$: let $C = \langle \pi_D \rangle Z(D^*)/Z(D^*)$, $U_0 = U_D Z(D^*)/Z(D^*)$ and for $i \geq 1$, $U_i = (1 + \mathbf{m}_D^i)Z(D^*)/Z(D^*)$.

Proposition 8.2. *The following holds:*

- (1) C is a cyclic group of order d .
- (2) U_0 is a normal subgroup of $\text{PGL}_1(D)$ and $\text{PGL}_1(D)$ is a semidirect product of U_0 by C .
- (3) For $i, j \geq 1$, U_i is a normal pro-2 subgroup of $\text{PGL}_1(D)$ and $[U_i, U_j] \leq U_{i+j}$. Moreover,

$$U_i/U_{i+1} \cong \begin{cases} \mathbb{F}_{q^d} & \text{if } i \not\equiv 0 \pmod{d} \\ \mathbb{F}_{q^d}/\mathbb{F}_q & \text{if } i \equiv 0 \pmod{d} \end{cases},$$

where $\mathbb{F}_{q^d} = (\mathbb{F}_{q^d}, +)$ denotes the additive group of the field.

- (4) U_0/U_1 is isomorphic to the multiplicative group of \mathbb{F}_{q^d} .

(5) Let $q = 2^r$ and $n = \dim_{\mathbb{Q}_2} K$. If $i > \frac{dn}{r}$ then $U_i^2 = U_{i+\frac{dn}{r}}$.

Proof. It is clear that (1) follows at once from the relations (8.1).

Since $\mathcal{O}_D = \mathcal{O}_K[w, \pi_D]$ and $w \in U_0$, we have that $\mathrm{PGL}_1(D) = U_0 C$. It is clear that U_0 is a normal subgroup of $\mathrm{PGL}_1(D)$ which intersects C trivially (because any power of π_D in $U_D Z(D^*)$ is already in $Z(D^*)$), so (2) follows.

The normality of the subgroups U_i and the statement on the commutator subgroups are straightforward. By [10, Proposition 1.8], the map $1 + a\pi_D^i \mapsto a + \mathbf{m}_D^i$ induces an isomorphism from $(1 + \mathbf{m}_D^i)/(1 + \mathbf{m}_D^{i+1})$ into the abelian group of the residue field $\mathcal{O}_D/\mathbf{m}_D \cong \mathbb{F}_{q^d}$. It follows from (1) that modding out by $Z(D^*)$ only affects the quotient group $(1 + \mathbf{m}_D^i)/(1 + \mathbf{m}_D^{i+1})$ when $i \equiv 0 \pmod{d}$, in which case $U_i/U_{i+1} \cong \mathbb{F}_{q^d}/\mathbb{F}_q$ because $(1 + \mathcal{O}_D \pi_D^i) \cap Z(D^*) = 1 + \mathcal{O}_K \pi_D^i$ and $\mathcal{O}_K \cap \mathbf{m}_D = \mathbf{m}_K$ (see Theorem 13.2 of [11]).

(4) follows from Proposition 1.8 of [10].

It remains to prove (5). The ramification index of K/\mathbb{Q}_2 is n/r by [11, Theorem 13.3], so we have that there exists a unit u of \mathcal{O}_K such that $u\pi_K^{n/r} = 2$. Now let $1 + a\pi_D^i \in (1 + \mathbf{m}_D^i) \setminus (1 + \mathbf{m}_D^{i+1})$, with $a \in U_D$. Then

$$(1 + a\pi_D^i)^2 = 1 + au\pi_D^{i+\frac{dn}{r}} + (a\pi_D^i)^2 \in 1 + \mathbf{m}_D^{i+\frac{dn}{r}},$$

since $i > \frac{dn}{r}$, and we easily deduce from the isomorphism $(1 + \mathbf{m}_D^i)/(1 + \mathbf{m}_D^{i+1}) \cong \mathcal{O}_D/\mathbf{m}_D$ used in the proof of (3) that

$$(1 + \mathbf{m}_D^i)^2 = (1 + \mathbf{m}_D^{i+\frac{dn}{r}}).$$

In particular, $U_i^2 = U_{i+\frac{dn}{r}}$. □

Corollary 8.3. *Let K be a finite extension of \mathbb{Q}_2 , D a K -central division algebra of dimension d^2 and $\mathcal{L} = \mathfrak{sl}_1(D)$. Assume that the Sylow pro-2 subgroups of $\mathrm{Aut}_{\mathbb{Q}_2}(\mathcal{L})$ are \mathbb{R} -finite. Then d is odd.*

Proof. Since \mathcal{L} is simple, the Sylow pro-2 groups of $\mathrm{Aut}_{\mathbb{Q}_2}(\mathcal{L})$ are just infinite (see Proposition III.9 of [8]). By Lemma 4.2, \mathbb{R} -finite just infinite pro-2 groups are torsion free, so $\mathrm{Aut}_K(\mathcal{L}) \subseteq \mathrm{Aut}_{\mathbb{Q}_2}(\mathcal{L})$ has no 2-torsion elements. Thus d must be odd by Proposition 8.1 and Proposition 8.2(1, 2). □

Corollary 8.4. *Let K be a finite extension of \mathbb{Q}_2 , D a K -central division algebra of dimension $d^2 > 1$ and $\mathcal{L} = \mathfrak{sl}_1(D)$. Assume that the Sylow pro-2 subgroups of $\mathrm{Aut}_{\mathbb{Q}_2}(\mathcal{L})$ have at most 25 real irreducible characters. Then $d = 3$ and $K = \mathbb{Q}_2$.*

Proof. Let $q = 2^r$ be the order of the residue field $\mathcal{O}_K/\mathbf{m}_K$ and $n = |K : \mathbb{Q}_2|$. Let $\rho \in \mathrm{Aut}_{\mathbb{Q}_2}(\mathcal{L})$. By Proposition 8.1, we may regard ρ as a \mathbb{Q}_2 -automorphism of D . Note that \mathcal{O}_D consists of integral over \mathbb{Z}_2 elements of D and so \mathcal{O}_D and \mathbf{m}_D are ρ -invariant. Then the restriction of ρ to \mathbf{m}_D^i induces an automorphism on the quotient $\mathbf{m}_D^i/\mathbf{m}_D^{i+1}$. If we identify $\mathbf{m}_D^i/\mathbf{m}_D^{i+1}$ with \mathbb{F}_{q^d} ($\mathbf{m}_D^i/\mathbf{m}_D^{i+1}$ is canonically isomorphic to $\mathcal{O}_D/\mathbf{m}_D \cong \mathbb{F}_{q^d}$), then ρ acts on $\mathbf{m}_D^i/\mathbf{m}_D^{i+1}$ as an element from $\mathrm{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_2) \ltimes \mathbb{F}_{q^d}^*$ acts on \mathbb{F}_{q^d} . Note that in this way we obtain a group homomorphism Ψ_i from $\mathrm{Aut}_{\mathbb{Q}_2}(\mathcal{L})$ into $\mathrm{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_2) \ltimes \mathbb{F}_{q^d}^*$.

Let P be a Sylow pro-2 subgroup of $\mathrm{Aut}_{\mathbb{Q}_2}(\mathcal{L})$. Since $|\mathrm{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_2) \ltimes \mathbb{F}_{q^d}^*| = rd(q^d - 1)$ and d is odd, by Corollary 8.3, we obtain that $|\Psi_i(P)| \leq r$. It follows

from this that the orbits of the action of a Sylow pro-2 group of $\text{Aut}_{\mathbb{Q}_2}(\mathcal{L})$ on $\mathbf{m}_D^i/\mathbf{m}_D^{i+1}$ have size at most r .

Next we consider the action of P on the subquotient $U_{\frac{dn}{r}}/U_{\frac{2dn}{r}}$ of $\text{PGL}_1(D) \cong \text{Aut}_K(\mathcal{L})$. For each $\frac{dn}{r} \leq i \leq \frac{2dn}{r} - 1$, P acts by conjugation on U_i/U_{i+1} . Recall that $w\pi_D^i + \mathbf{m}_D^{i+1} \mapsto (1 + w\pi_D^i)U_{i+1}$ defines a group homomorphism from $\mathbf{m}_D^i/\mathbf{m}_D^{i+1}$ onto U_i/U_{i+1} , and it is easy to check that this map respects the action of P . It follows that the P -orbits in U_i/U_{i+1} have size at most r and so by Proposition 8.2(3),

$$r_P((U_i \setminus U_{i+1})/U_{i+1}) \geq \begin{cases} \frac{q^d-1}{q^{\frac{r}{d}-1}} & \text{if } i \not\equiv 0 \pmod{d} \\ \frac{q^{\frac{r}{d}-1}-1}{r} & \text{if } i \equiv 0 \pmod{d} \end{cases}.$$

Thus, we obtain that

$$r_P(U_{\frac{dn}{r}}/U_{\frac{2dn}{r}}) \geq 1 + \sum_{i=\frac{dn}{r}}^{\frac{2dn}{r}-1} r_P((U_i \setminus U_{i+1})/U_{i+1}) \geq \frac{n}{r^2}((d-1)(2^{rd}-1) + 2^{r(d-1)} - 1) + 1.$$

Since $r_P(U_{\frac{dn}{r}}/U_{\frac{2dn}{r}}) \leq 25$ and d is odd, an easy calculation yields to $d = 3$ and $n = 1$. □

The following theorem implies Theorem B.

Theorem 8.5. *Let D be a \mathbb{Q}_2 -central division algebra of dimension 9 and $\mathcal{L} = \mathfrak{sl}_1(D)$. Then the Sylow pro-2 subgroups of $\text{Aut}_{\mathbb{Q}_2}(\mathcal{L})$ have exactly 25 real irreducible characters.*

Proof. By Proposition 8.1 and by the Skolem-Noether theorem,

$$\text{Aut}_{\mathbb{Q}_2}(\mathcal{L}) \cong \text{Aut}_{\mathbb{Q}_2}(D) \cong \text{PGL}_1(D) = D^*/Z(D^*).$$

When there is no possible confusion, we shall identify an element in the group $\text{Aut}_{\mathbb{Q}_2}(\mathcal{L})$ with a preimage of it in D .

Using the same notation as at the beginning of the section, let w be a primitive 7th root of unity, and π_D an element such that $\pi_D^3 = 2 \in \mathbb{Z}_2$ and $(\pi_D)^{-1}w\pi_D = w^2$, so we can assume that

$$D = \mathbb{Q}_2[w, \pi_D].$$

Recall that the valuation ring $\mathcal{O}_D = \mathbb{Z}_2[w, \pi_D]$ has a unique maximal ideal $\mathbf{m}_D = \pi_D \mathcal{O}_D$, and it is clear that $2\mathcal{O}_D = \mathbf{m}_D^3$ and $\mathcal{O}_D/\mathbf{m}_D \cong \mathbb{F}_8$. We know that the group U_1 defined above is a Sylow pro-2 subgroup of $\text{PGL}_1(D)$.

We start with some calculations inside the group U_1 .

Claim 1. *Let $i, j \geq 1$ and $x \in U_i \setminus U_{i+1}$. Then $C_{U_j}(xU_{i+j+1}) = C_{U_j}(x)U_{j+1}$.*

Proof. The inclusion $C_{U_j}(x)U_{j+1} \leq C_{U_j}(xU_{i+j+1})$ is obvious. Let us show the converse inclusion. Write $i = i_0 + 3i_1$ and $j = j_0 + 3j_1$ with $0 \leq i_0, j_0 \leq 2$. The proof is divided in 4 subcases depending on whether i_0 and j_0 are equal or not to 0. We consider only the subcase when $i_0, j_0 \neq 0$, the other cases are proved similarly.

We write $x \equiv 1 + a\pi_D^i \pmod{U_{i+1}}$ with $a \in \mathcal{O}_D \setminus \mathbf{m}_D$. First observe that since $i_0, j_0 \neq 0$, $|C_{U_j}(x)U_{j+1}/U_{j+1}| \geq 2$. Indeed, if $i_0 = j_0$, then $1 + a\pi_D^i 2^{j_1-i_1} \in C_{U_j}(x) \setminus U_{j+1}$ and if $i_0 \neq j_0$, then $1 + (a\pi_D)^{2i_0(j-2i_0)/3} \in C_{U_j}(x) \setminus U_{j+1}$.

Thus, it is enough to show that $|C_{U_j}(xU_{i+j+1})/U_{j+1}| = 2$. Take $y \in C_{U_j}(xU_{i+j+1})$ with $y \equiv 1 + b\pi_D^j \pmod{U_{j+1}}$ and $b \in \mathcal{O}_D \setminus \mathbf{m}_D$. Since $[x, y] \in U_{i+j+1}$ we obtain that $ab^{4^i} - ba^{4^j} \in \mathbf{m}_D$. Hence

$$(8.2) \quad b^{4^i-1} \equiv a^{4^j-1} \pmod{\mathbf{m}_D}.$$

Recall that $\mathcal{O}_D/\mathbf{m}_D \cong \mathbb{F}_8$. Note that the map $\mathbb{F}_8^* \rightarrow \mathbb{F}_8^*$ that sends \bar{b} to $\bar{b}^{2^{2i}-1}$ is a bijection, since $i \not\equiv 0 \pmod{3}$. Hence there exists only one class of b modulo \mathbf{m}_D that satisfies (8.2). This implies that $|C_{U_j}(xU_{i+j+1})/U_{j+1}| = 2$. \square

As a corollary we obtain the following.

Claim 2. *Let $i, j \geq 1$, $n > i + j$ and $x \in U_i \setminus U_{i+1}$. Then $C_{U_j}(xU_n) = C_{U_j}(x)U_{n-i}$.*

Proof. The proof is done by induction on n . The base of induction ($n = i + j + 1$) is done in the previous claim. \square

By Proposition 8.2(5), U_i/U_{i+3} is elementary abelian for $i \geq 4$. Thus all the conjugacy classes in this group are real. Moreover, the same result implies that these are all the conjugacy classes of elements of order at most 2 in U_i/U_{i+3} . In the following claim we count their number.

Claim 3. *Let $i \equiv 1 \pmod{3}$ and assume $i \geq 4$. Then $r_{U_1}(U_i/U_{i+3}) = 25$.*

Proof. Recall that U_{i+2}/U_{i+3} is central in U_1/U_{i+3} . By Claim 2, if $x \in U_i \setminus U_{i+1}$, then $C_{U_1}(xU_{i+3}) = C_{U_1}(x)U_3$ and if $x \in U_{i+1} \setminus U_{i+2}$ then $C_{U_1}(xU_{i+3}) = C_{U_1}(x)U_2$. Moreover, using that $i \equiv 1 \pmod{3}$, an argument along the lines of the proof of Claim 1 yields that if $x \in U_i \setminus U_{i+1}$ then $|U_1 : C_{U_1}(x)U_3| = 2^4$, and if $x \in U_{i+1} \setminus U_{i+2}$ then $|U_1 : C_{U_1}(x)U_2| = 2^2$.

By the previous paragraph, since $i \equiv 1 \pmod{3}$ we have that Proposition 8.2(3) implies that there are $14 = \frac{|(U_i \setminus U_{i+1})/U_{i+3}|}{2^4}$ U_1 -conjugacy classes in $(U_i \setminus U_{i+1})/U_{i+3}$, $7 = \frac{|(U_{i+1} \setminus U_{i+2})/U_{i+3}|}{2^2}$ U_1 -conjugacy classes in $(U_{i+1} \setminus U_{i+2})/U_{i+3}$ and $4 = |U_{i+2}/U_{i+3}|$ U_1 -conjugacy classes in U_{i+2}/U_{i+3} . \square

By the comments before Claim 3, in order to finish the proof we only need to show that for large i , U_1/U_i does not contain real elements of order 4.

Claim 4. *Let $i \geq 4$. Let $x \in U_i$ be such that xU_{i+4} is a real element of order 4 in U_1/U_{i+4} . Then there exists $y \in U_3$ such that $(xU_{i+4})^y = (xU_{i+4})^{-1}$.*

Proof. Note that $x^2 \in U_{i+3}$ by Proposition 8.2(5). Now if $y \in U_1$ is such that $(xU_{i+4})^y = (xU_{i+4})^{-1}$, then $y \in C_{U_1}(xU_{i+3})$, and thus by Claim 2 we can assume that $y \in U_3$. \square

Claim 5. *If $i \geq 6$, then there are no real elements of order 4 in U_1/U_{i+4} .*

Proof. Let xU_{i+4} be a real element of order 4 in U_1/U_{i+4} . Then $x \in U_j \setminus U_{j+1}$ for $i - 2 \leq j \leq i$. Since the following arguments do not depend on the value of j , for simplicity we may assume that $x = 1 + a\pi_D^i \in U_i$ with $a \in \mathcal{O}_D \setminus \mathbf{m}_D$. Again we distinguish two cases depending on whether $i \equiv 0 \pmod{3}$ or not. We only consider the case $i \not\equiv 0 \pmod{3}$, the other case is proven in a similar way.

By the previous claim there exists $y = 1 + 2b \in U_3$ ($b \in \mathcal{O}_D \setminus \mathbf{m}_D$) such that

$$1 + 2(ab^{4^i} - ab)\pi_D^i \equiv [x, y] \equiv x^2 \equiv (1 + 2a\pi_D^i) \pmod{U_{i+4}}.$$

Hence $ab^{4^i} - ab \equiv a \pmod{\mathfrak{m}_D}$. Since a is invertible in \mathcal{O}_D , we obtain that there should exist $\bar{b} \in \mathbb{F}_8 \cong \mathcal{O}_D/\mathfrak{m}_D$ such that $\bar{b}^{2^{2^i}} - \bar{b} = \bar{1}$. But this is impossible, obtaining a contradiction. \square

Now we are ready to finish the proof of the theorem. Let i be a positive integer congruent to 1 modulo 3. It suffices to prove that for any large enough i , the finite 2-group U_1/U_i has 25 real conjugacy classes, by Lemma 2.4 and Lemma 4.2(2). This follows from Claims 3 and 5. \square

9. PROOF OF THEOREM A

In this section we obtain Theorem A as a consequence of two results. Firstly we show that if there are infinitely many finite 2-groups G as in the statement of Theorem A, then there is an infinite pro-2 group having exactly r real irreducible characters. Secondly we show that such a pro-2 group does not exist for odd r and $r \leq 23$.

Theorem 9.1. *Let r be a natural number. Assume that there are infinitely many finite 2-groups G with $r(G) = r$. Then there is an infinite pro-2 group having exactly r real irreducible characters*

Proof. Let us consider the following directed graph Γ . The set of vertices $V(\Gamma)$ of Γ consists of the isomorphism classes of finite 2-groups with exactly r real irreducible conjugacy classes. There is an edge from G_1 to G_2 if and only if there exists a normal subgroup Z of order 2 in G_2 such that $G_2/Z \cong G_1$. We say also that G_1 is a father of G_2 and G_2 is a son of G_1 .

Claim 1. *There is a number C , such that if $G \in V(\Gamma)$ and $|G| > C$, then G has at least one father.*

Proof. Let $G \in V(\Gamma)$. By Lemma 2.7(3), there exists an r -bounded k such that $\text{Irr}_r(G/G_k) = \text{Irr}_r(G)$. Note that the order of G_i/G_{i+1} is r -bounded for all $1 \leq i \leq k-1$ by Lemma 2.7(1), whence the order of G/G_k is also r -bounded (say $|G/G_k| \leq C = C(r)$). Thus, if $|G| > C$ then $G_k \neq \{1\}$. Let $Z \leq G_k$ be a normal subgroup of G of order 2. Then it is clear that G/Z is a father of G . \square

For any $G \in V(\Gamma)$ consider the subgraph Γ_G of Γ consisting of G and all its descendants (the vertices of Γ that can be reached by a path from G).

Claim 2. *Let $2^n \geq C$. Then there exists a group $G \in V(\Gamma)$ of order 2^n , such that Γ_G is infinite. Moreover, if $H \in V(\Gamma)$ and Γ_H is infinite, then there exists a son G of H such that Γ_G is infinite.*

Proof. From the previous claim any group in $V(\Gamma)$ of order at least 2^n lies in $\cup_{G \in V(\Gamma), |G|=2^n} \Gamma_G$. Thus if Γ is infinite, then some Γ_G is infinite. The second statement of the claim is proved in a similar way. \square

Now we are ready to finish the proof of the theorem. By the previous claim we can construct inductively $G_i \in V(\Gamma)$, $i \in \mathbb{N}$, such that Γ_{G_i} is infinite and G_{i+1} is a son of G_i . Then the pro-2 group isomorphic to the inverse limit of $\{G_i\}_{i \in \mathbb{N}}$ has exactly r real irreducible characters. \square

Theorem 9.2. *Let P be a pro-2 group having r real irreducible characters. If r is odd and $r \leq 23$, then P is finite.*

Proof. By way of contradiction, assume that there exists an infinite pro-2 group P having an odd number of real irreducible characters smaller than 25. Then P is of finite rank. Thus, we may assume also that $\dim \mathcal{L}(P)$ is as small as possible. If P is not just infinite, by Corollary 5.2, any of its just infinite quotients satisfies our hypothesis. Thus, assume also that P is just infinite. Then P is an open subgroup of $\text{Aut}(\mathcal{L})$, where $\mathcal{L} = \mathcal{L}(P)$ is a semi-simple finite dimensional Lie \mathbb{Q}_2 -algebra all whose simple components are isomorphic. Also, by Corollary 5.3 P is non-solvable. Note also that P is torsion free, because all torsion elements of P are in $\text{rad}_f(P)$ (Lemma 4.2(3)).

If P is not a Sylow pro-2 subgroup of $\text{Aut}(\mathcal{L})$, then there exists $P < Q \leq \text{Aut}(\mathcal{L})$ such that $|Q : P| = 2$. By Theorem 6.1, there exists $a \in Q$ such that $C_P(a)$ has an odd number of real characters and $|\text{Irr}_r(C_P(a))| \leq |\text{Irr}_r(P)|$. Observe that a acts non-trivially on \mathcal{L} and so the dimension of $\mathcal{L}(C_P(a)) \cong \mathcal{L}(a)$ is smaller than the dimension of \mathcal{L} . This contradicts to our choice of P .

On the other hand, if P is a Sylow pro-2 subgroup of $\text{Aut}(\mathcal{L})$ then, by Theorem 7.1, $\mathcal{L}(P) \cong \mathfrak{sl}_1(D)$ for some division \mathbb{Q}_2 -algebra D . Corollary 8.4 implies that D has dimension 9 over its center \mathbb{Q}_2 . But then Theorem 8.5 states that $|\text{Irr}_r(P)| = 25 > 23$, a contradiction. \square

10. FURTHER COMMENTS

In this section we describe several possible directions for further research. As we have proved the “minimal” pro-2 group with odd number of conjugacy classes belong to the Sylow subgroups of $\text{PGL}_1(D)$ where D has dimension at least 9 over its center. In particular, these groups have at least 3 generators. So we suggest the following problem.

Conjecture 1. *Let k be an odd number. Then there exists only a finite number of finite 2-groups generated by 2 elements with exactly k real conjugacy classes.*

In a similar fashion to Lemma 4.2 we believe that the following holds.

Conjecture 2. *Let G be a finite 2-group. Then $\text{rk}(G)$ is q -bounded, where q is the number of rational characters of G .*

REFERENCES

1. N. Bourbaki, *Lie groups and Lie algebras*, Chapters 1–3, Springer-Verlag, Berlin, 1998.
2. N. Bourbaki, *Lie algebras and Lie groups*, Chapters 7–9, Springer-Verlag, Berlin, 2005.
3. J. D. Dixon; M. P. F. du Sautoy; A. Mann; D. Segal, *Analytic pro- p groups*, Second edition, Cambridge University Press, Cambridge, 1999.
4. J. E. Humphreys, *Linear algebraic groups*, Springer-Verlag, New York-Heidelberg, 1975.
5. I. M. Isaacs, *Character Theory of Finite Groups*, Academic Press Inc., New York, 1976.
6. I. M. Isaacs; G. Navarro; J. Sangroniz, p -groups having few almost-rational irreducible characters, *Israel J. Math.* **189** (2012), 65–96.
7. N. Jacobson, *Lie algebras*, Dover Publications, Inc., New York, 1979.
8. G. Klaas; C. R. Leedham-Green; W. Plesken, *Linear pro- p -groups of finite width*, Springer-Verlag, Berlin, 1997.
9. M. Kneser, Galois-Kohomologie halbeinfacher algebraischer Gruppen über p -adischen Körpern I, II, *Math. Z.* **88** (1965) 40–47; **89** (1965) 250–272.
10. V. Platonov; A. Rapinchuk, *Algebraic groups and number theory*, Academic Press, Inc., Boston, MA, 1994.
11. I. Reiner, *Maximal orders*, Academic Press Inc., London, 1975.

12. J. Sangroniz; J. Tent, 2-groups with a fixed number of real conjugacy classes, *J. Algebra* **392** (2013), 42–51.
13. J.-P. Serre, *Local fields*, Springer-Verlag, New York-Berlin, 1979.
14. L. Ribes; P. Zalesskii, *Profinite groups*, Second edition, *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics*, 40, Springer-Verlag, Berlin, 2010.
15. D. J. S. Robinson, *A course in the theory of groups*, Second edition, Graduate texts in mathematics, Springer-Verlag New York, Inc. 1995.
16. J. Rotman, *An introduction to the theory of groups*, Springer-Verlag, New York, 1995.

DEPARTAMENTO DE MATEMÁTICAS, UNIVERSIDAD AUTÓNOMA DE MADRID, AND INSTITUTO DE CIENCIAS MATEMÁTICAS - CSIC, UAM, UCM, UC3M. 28049 MADRID, SPAIN.

E-mail address: `andrei.jaikin@uam.es`

DEPARTAMENT D'ÀLGEBRA, UNIVERSITAT DE VALÈNCIA. 46100 BURJASSOT, VALÈNCIA, SPAIN.

E-mail address: `joan.tent@uv.es`